UNITED STATES DISTRICT COURT

for the

Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2610 Plaza Court, #107,
High Point, North Carolina 27263

Case No. 1:25MJ70

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A to the accompanying Affidavit.

located in the Middle District of North Carolina, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B to the accompanying Affidavit.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
7 U.S.C. § 2024; 18 U.S.C. §§ 641; 1029; and 1343	Fraud associated with the Supplemental Nutrition Assistance Program; theft of public money; access device fraud; and wire fraud

The application is based on these facts:

See accompanying Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Michael Johnson
Applicant's signature

Michael Johnson, Special Agent, USDA-OIG
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 03/04/25

Judge's signature

City and state: Greensboro, North Carolina

The Hon. L. Patrick Auld, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael Johnson, Special Agent with the United States Department of Agriculture, Office of Inspector General, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant authorizing the search of APNA HALAL MEATS (hereinafter "AHM"), 2610 Plaza Court, #107, High Point, North Carolina 27263 (hereinafter the "SUBJECT PREMISES"), which is located in the Middle District of North Carolina and as more fully described in Attachment A.

2. Based on my training and experience and the facts as set forth in this affidavit, your affiant has probable cause to believe that the owner, Mohammad Azam KHAN (hereinafter "KHAN") is using the SUBJECT PREMISES to engage in fraud associated with the Supplemental Nutrition Assistance Program, in violation of 7 U.S.C. § 2024; access device fraud, in violation of 18 U.S.C. § 1029; theft of public money, in violation of 18 U.S.C. § 641; and wire fraud, in volitation of 18 U.S.C. § 1343. Your affiant further believes evidence, instrumentalities, and fruits of such violations, as described in Attachment B, will be located at the SUBJECT PREMISES.

II. AGENT BACKGROUND

3. I have been employed as a Federal Law Enforcement Officer for nearly twelve years. During this time, I have participated in and/or conducted investigations in a wide variety of matters, such as human trafficking, sex trafficking, child exploitation, defrauding of

Government benefit programs, cattle and livestock theft, dogfighting and cock fighting, narcotics trafficking, human smuggling, customs violations, maritime smuggling, and more.

4. I am currently a Special Agent with the United States Department of Agriculture, Office of Inspector General (USDA-OIG), and have been in this position since April 2020. Prior to my current position with USDA-OIG, I was employed as a federal law enforcement officer for over seven years within the Department of Homeland Security; approximately two and half years as a Special Agent with Homeland Security Investigations, and nearly four and a half years as an Agent with the United States Border Patrol. Additionally, I served in the United States Coast Guard Reserves as a Petty Officer, obtaining the rate of Boatswain's Mate Third Class.

5. I have attended training in various aspects of law enforcement techniques and criminal investigations at two of the Federal Law Enforcement Training Center (FLETC) facilities, located in Artesia, New Mexico, and Glynco, Georgia. I successfully graduated from the United States Border Patrol Academy, FLETC's Criminal Investigator Training Program, and the Homeland Security Investigations' Special Agent Training Program.

6. As part of my duties as a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States. My duties and responsibilities include the investigation of crimes that affect the operations and programs of the USDA, including Supplemental Nutrition Assistance Program fraud, theft of Government property, wire fraud, access device fraud, money laundering, and other related financial crimes. I have participated in investigations of such crimes, and I have received specialized training in the investigation these offenses and related Title 7 and Title 18 offenses.

7. I am familiar with the facts set forth herein based on my personal observations and information provided to me by other law enforcement personnel participating in this investigation.

I am also familiar with the facts set forth based on my review of documents, reports, photographs, and video files.

8. As the purpose of this affidavit is only to establish probable cause to support the issuance of search and seizure warrants, I have not set forth each and every fact known concerning this investigation. Where statements of others are set forth in this affidavit, they are set forth in substance and in part. In addition, the events described in this affidavit occurred on or about the dates provided herein.

III. THE SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM

9. The Supplemental Nutrition Assistance Program ("SNAP"), formerly known as the Food Stamp Program, is a federally funded nation-wide program that the United States established to alleviate hunger and malnutrition among lower income families. The USDA administers the SNAP through its agency, the Food and Nutrition Service ("FNS"). The FNS is responsible for the authorization and disqualification of retail food establishments participating in the redemption of SNAP benefits. Social service agencies from each state share responsibility with FNS for the administration of the program by authorizing and revoking distribution of SNAP benefits to individual recipients.

10. In North Carolina, the North Carolina Department of Health and Human Services ("NCDHHS") administers this program. Beginning in 1990, USDA FNS and state agencies administering the SNAP program began the transition process from a traditional paper coupon system to an Electronic Benefit Transfer ("EBT") card system. The nationwide transition to EBT cards was completed in 2004.[1] NCDHHS awarded Fidelity Information Services ("FIS") the current network management contract for North Carolina's EBT system. The system is similar to

[1] *A Short History of SNAP,* https://www.fns.usda.gov/snap/history

that involved with the use of debit and credit cards. SNAP recipients receive a plastic EBT card that contains an embedded magnetic stripe that stores account information necessary to conduct food purchases. Stores approved by FNS to participate in the SNAP program receive an assigned SNAP authorization number. They must contract with a payment processor and acquire a point of sale ("POS") terminal in order to access the electronic funds allocated to recipients' EBT cards. The POS terminal communicates with an authorization platform to debit a recipient's available SNAP benefit balance for the cash value of eligible food items that the SNAP recipient purchases.

11. When a customer swipes an EBT card through a retailer's POS terminal, a store employee must actively select "SNAP/food stamp purchase" as the transaction type from the POS terminal menu. These transactions can also be completed by manually entering the EBT card's number into the terminal. The employee must then enter the total dollar amount of the transaction to occur. The transaction request is complete when the cardholder enters his/her unique personal identification number ("PIN"). This causes an electronic transmission of information through a series of business supporting networks. The POS terminal communicates through the retailer's payment processor to the FIS authorization platform, which is co-located in data centers in Arizona and Wisconsin. This is where online recipient information is maintained. The authorization platform verifies that the retailer is authorized to process the SNAP transaction by looking up its status in a retailer database. It then verifies the number of benefits available, authorizes the transaction, and deducts the purchase amount from the SNAP recipient's available balance. The system also calculates cumulative SNAP sales for each retailer and authorizes electronic payments to the retailer's bank account.

12. Upon the approval of the transaction, information flows back to the POS terminal and the store employee receives confirmation that the cardholder's account has been successfully

debited. Unlike the procedures for the original paper food stamp coupons, SNAP EBT transactions are for the exact amount of the sale and the cardholder gets no change back. SNAP reimbursements go to authorized retailers through a series of electronic funds transfers.

13. In order to participate in the SNAP as an authorized retailer, a business must complete FNS Form 252 (Supplemental Nutrition Assistance Program Application for Stores) via an online application system. The owner/manager of the business must acknowledge receiving mandatory SNAP retailer training. This training from FNS educates and trains store owner/management personnel on the proper procedures for the acceptance and redemption of SNAP benefits. Training materials are in English and Spanish and are available online. In addition, a qualified storeowner must acknowledge his receipt of those training materials in his application packet and the packet specifically warns that if the owner does not receive those materials, he must contact the FNS for copies of them. Store owners/managers are responsible for training their employees in the proper procedures for the program. In fact, within the "Electronic Application" that KHAN, the owner of AHM, sent to the USDA in February 2018, was an acknowledgement that it was his "responsibility to ensure that the training materials are reviewed by all firm's owners and all employees." Retailers may lose their authorization to redeem SNAP benefits if they break program rules or no longer qualify for participation in the program. The documentation also warned of possible "criminal prosecution and sanctions" for acts such as "[t]rading cash for Supplemental Nutrition Assistance Program benefits" (i.e. trafficking) and "[a]ccepting Supplemental Nutrition Assistance Program benefits as payment for ineligible items."

14. Pursuant to the Food and Nutrition Act and regulations that the Secretary of Agriculture promulgated under it, SNAP authorized retailers may only accept SNAP benefits in exchange for eligible food items. SNAP benefits may not in any case be exchanged for cash (a

practice commonly referred to as trafficking) or for other forbidden items such as alcohol, tobacco products, lottery tickets, or fuel.

IV. SUPPLEMENTAL NUTRITION ASSISTANCE PROGRAM TRAFFICKING AND FRAUD

15. Your affiant knows from training and experience that a common form of SNAP trafficking involves an exchange of cash for SNAP benefits between a retailer that has been approved by FNS to accept SNAP, and a SNAP benefit recipient. In this form of trafficking, the retailer will provide the cash to the recipient at an agreed to rate (commonly fifty cents of cash per SNAP benefit dollar, though the rate may vary) and then submit a SNAP transaction through the retailer's POS terminal as if a legitimate SNAP-eligible purchase had occurred. A purchase of SNAP-eligible or ineligible items may occur during the trafficking transaction.

16. These transactions are often completed with the recipient and their EBT card present at the store but can also occur without the recipient or their card being present. Recipients may leave their card at the retailer for extended periods of time, allowing the retailer to swipe the card through the POS terminal. The retailer then provides the cash to the recipient at a later time in person or pays the recipient via a person-to-person payment application, such as Cash App or Venmo. A "manual" transaction may occur if the EBT card number and PIN are provided to the retailer, often via text message or another cell phone messaging application, along with a desired amount of cash the recipient wishes to receive. The retailer can then manually type in the EBT card's number and PIN into the POS terminal without physically possessing the EBT card. Previous investigative operations known to your affiant and other USDA-OIG Agents have demonstrated this pattern of fraudulent activity in the past.

17. Stores participating in SNAP trafficking often refer to the difference between the amount of the transaction the EBT card is debited for and the cash paid to the recipient as a "fee."

18. For example, if a recipient has a balance of $500.00 on their EBT card, they may visit the store and select $26.00 worth of items they wish to purchase from the store; the eligibility of the items selected for purchase is often irrelevant during trafficking transactions. The recipient would then approach the clerk operating the register with an EBT POS terminal and request $200.00 cash in addition to the $26.00 of items they wish to purchase. If the agreed upon exchange rate of SNAP benefits for cash is fifty cents per dollar of SNAP benefits, the clerk would process a transaction through the POS terminal for $426.00 ($200 cash + $200 fee + $26 of items).

V. APNA HALAL MEATS STORE HISTORY

19. A search of North Carolina Secretary of State records revealed that Mohammad Azam KHAN completed North Carolina Secretary of State Form B-01, Articles of Incorporation, on January 30, 2018, for a corporation named "PAK MK FAMILY, Inc." This form listed KHAN as the initial registered agent, as the sole incorporator, and was signed by KHAN at the bottom with the title "President/Incorporator." On the form, the initial registered office of the corporation, the address of the principal office of the corporation, and KHAN's address as an incorporator are all listed as "2610 PLAZA CT STE 107, HIGH POINT, NC 27263," the same address as AHM and the SUBJECT PREMISES.

20. According to North Carolina Secretary of State records, "PAK MK FAMILY, Inc" was incorporated on February 2, 2018, and assigned Secretary of State ID Number 1661214.

21. According to the FNS 252 on file for AHM, KAHN completed the application on or about March 20, 2018. The store name provided on the FNS 252 was "Apna Halal Meats." Also on the form is a section requiring applicants to list the name of the corporation on record with the State, which KHAN provided as "Pak Mk Family Inc." The SUBJECT PREMISES was provided as the address for the store location address and the corporation address.

22. FNS approved AHM's application to accept SNAP benefits on April 26, 2018, and assigned AHM FNS store number 0630881. The first SNAP transaction at AHM occurred on May 8, 2018.

23. As of November 13, 2024, the records for "PAK MK FAMILY, Inc" show KHAN as the registered agent and the SUBJECT PREMISES as the mailing and principal office address. However, the President is now listed as "MOHAMMAD AZAM KHAN, WANA P.L.L.C."

24. According to records on file with FNS, AHM is classified as a medium grocery store. FNS provides a store code abbreviation of "MG" for medium grocery stores and defines them as "[a] store that carries a moderate selection of all four staple food categories. They may sell ineligible items as well, but their primary stock is food items."[2]

VI. PROBABLE CAUSE

25. Based on the facts listed herein, there is probable cause to believe that KHAN committed criminal violations of the United States Code. There exists probable cause to believe that within the premises of AHM is evidence of the commission of a crime, contraband, the fruits of a crime or things otherwise criminally possessed, and instrumentalities of numerous federal offenses to include fraud associated with the Supplemental Nutrition Assistance Program, in violation of 7 U.S.C. § 2024; access device fraud, in violation of 18 U.S.C. § 1029, theft of public money, in violation of 18 U.S.C. § 641; and wire fraud, in volitation of 18 U.S.C. § 1343. This belief stems from materials uncovered during investigations as set forth below.

A. Apna Halal Meats Transaction History

26. According to FNS data, during the period from May 2018 to January 2025, AHM redeemed a total of $5,439,613.55 in SNAP benefits. During the same period medium grocery

[2] *SNAP Store Type Definitions,* https://www.fns.usda.gov/snap/store-definitions

stores[3] authorized to accept SNAP benefits in Guilford County, the county in which AHM is located, redeemed a collective average of $1,196,502.78 in SNAP benefits. The average amount of SNAP benefits redeemed by all medium grocery stores in the state of North Carolina during the same period was $614,358.86.

27. During the same May 2018 to January 2025 period, AHM processed 56,128 SNAP purchase transactions, compared to a collective average of 22,992 for medium grocery stores in Guilford County, and a collective average of 15,816 for all medium grocery stores in the state of North Carolina.

28. During the same May 2018 to January 2025 period, the average SNAP transaction amount at AHM was $96.91, compared to a collective average SNAP transaction of $52.04 for medium grocery stores in Guilford County, and a collective average SNAP transaction of $38.84 for all medium grocery stores in the state of North Carolina. AHM's average SNAP transaction of $96.91 exceeds the average SNAP transaction of $46.58[4] for stores designated as Supermarkets by FNS in Guilford County, such as Publix, Food Lion, Aldi, and Lowes Food.

29. During the month of June 2018, the store's first full month of conducting SNAP transactions,[5] $23,769.50 in SNAP benefits were redeemed at AHM. From July 2018 to April 2020, monthly redemptions ranged from $16,892.66 to $32,442.23, all of which were higher than the monthly dollar redemptions for medium grocery stores in Guilford County during the same months. Beginning in March 2021 and in the following ten months, AHM's monthly SNAP redemptions were $90,000.00 or greater. SNAP redemptions climaxed in August 2021, during

[3] The county and state averages provided include AHM's transactional data.
[4] The average SNAP transaction amount for Supermarket stores in Guilford County is based on data from May 2018 to November 2024. FNS data for Supermarkets for December 2024 was not available at the time of writing.
[5] AHM's first transaction occurred on May 8, 2018, according to FNS data.

which AHM redeemed $239,048.25 worth of SNAP benefits, with an average SNAP transaction amount of $175.26.

30. Based on the fraud loss calculation method utilized by USDA-OIG during federal SNAP fraud investigations,[6] the estimated fraud loss to the SNAP program from transactions conducted at AHM from May 2018 to January 2025 is $4,243,110.77.

Store Name	Total SNAP Dollar Volume	SNAP Volume % Difference	Average SNAP Transaction	Average Transaction % Difference
Apna Halal Meats	$5,439,613.55	-	$96.91	-
MG in Guilford	$1,196,502.78	354.63%	$52.04	86.22%
MG in all NC	$615,358.86	785.41%	$38.84	149.51%
Estimated Fraud	**$4,243,110.77**			

Table comparing SNAP transaction volume and average SNAP transaction amount between Apna Halal Meats, medium grocery stores in Guilford County ("MG in Guilford"), and all medium grocery stores in the state of North Carolina ("MG in all NC"). Data is drawn from FNS for May 2018 to January 2025.[7]

31. Your affiant conducted a detailed review of AHM's EBT transactions conducted since the store was authorized to accept SNAP benefits and found transactions, patterns, and data consistent with those commonly seen at retailers conducting SNAP trafficking. Samples of these transactions are detailed below.

Balance Depletion Transactions

32. Your affiant knows from training and experience conducting SNAP trafficking investigations that retailers will often deplete the balance of EBT cards in a manner designed to make the trafficking transactions less likely to be detected by FNS and law enforcement. For example, if an EBT card has a balance of $3,000 in SNAP benefits, a store may complete multiple transactions through their EBT POS terminal in various increments to avoid having a single $3,000

[6] The formula for calculating fraud loss as a result of SNAP trafficking is *(SNAP redemption total of the subject store during the time period) - (average SNAP redemption total for stores with the same FNS classification, in the same county, during the same period).*

[7] The county and state averages provided include AHM's transactional data.

EBT transaction at the store, which would be more likely to be scrutinized. Your affiant has located transaction patterns consistent with this methodology of trafficking.

33. On January 25, 2023, an EBT card with a starting SNAP benefits balance of $4,060.43 was swiped through AHM's POS terminal four times, all within one minute and forty-three seconds of each other, totaling $3,743.37 in EBT transactions.

a. On January 25, 2023, at 12:28:26 PM, the EBT card was swiped through AHM's POS terminal for $996.29.

b. On January 25, 2023, at 12:28:58 PM, 32 seconds after the previous transaction, the EBT card was swiped through AHM's POS terminal for $769.55.

c. On January 25, 2023, at 12:29:29 PM, 31 seconds after the previous transaction, the EBT card was swiped through AHM's POS terminal for $1,207.85.

d. On January 25, 2023, at 12:30:09 PM, 40 seconds after the previous transaction, the EBT card was swiped through AHM's POS terminal for $769.68.

34. Based on your affiant's knowledge of SNAP trafficking patterns, AHM and the SNAP eligible items within the store, the average transaction amount for medium grocery stores in Guilford County, and general life experience shopping for groceries, your affiant believes these EBT transactions are fraudulent. This is based on your affiant's belief that it is unlikely that an EBT cardholder purchased $3,743.37 worth of items at AHM; it is unlikely that an employee at AHM could ring up and process $3,743.37 worth of items through their checkout in one minute and forty-three seconds; it would be an uncommon practice to break up a legitimate transaction into four separate transactions. These transactions are summarized below:

Date	Time	Amount	Prior Balance	Ending Balance
01/25/2023	12:28:26 PM	$996.29	$4,060.43	$3,064.14
01/25/2023	12:28:58 PM	$769.55	$3,064.14	$2,294.59
01/25/2023	12:29:29 PM	$1,207.85	$2,294.59	$1,086.74

01/25/2023	12:30:09 PM	$769.68	$1,086.74	$317.06

Table summarizing the transactions described in paragraphs 35 through 36.

35. Your affiant located transactions at AHM in which an EBT card's balance was depleted of most of its balance in single transactions instead of multiple transactions described above. Your affiant theorizes that these depletions occurred in single transactions because AHM believed the lower balance on the EBT card was less likely to be detected than the larger balance in the transactions detailed above.

36. On May 6, 2022, an EBT card with a starting SNAP benefits balance of $2,492.98 was swiped through AHM's POS terminal for a $2,492.95 EBT transaction, leaving a remaining balance of $0.03.

37. On April 19, 2024, an EBT card with a starting SNAP benefits balance of $1,044.54 was swiped through AHM's POS terminal two times in two minutes and eight seconds, totaling $1,032.15 in EBT transactions.

a. On April 19, 2024, at 10:08:06 AM, the EBT card was swiped through AHM's POS terminal for a 'Balance Inquiry,' which provides the retailer and the cardholder with the balance of benefits remaining on the card. The balance of the card was $1,044.54.

b. On April 19, 2024, at 10:10:14 AM, two minutes and eight seconds after the balance inquiry, the EBT card was swiped through AHM's POS terminal for $1,032.15. These transactions are summarized below:

Date	Time	Amount	Prior Balance	Ending Balance
04/19/2024	10:08:06 AM	Balance Inquiry	$1,044.54	$1,044.54
04/19/2024	10:10:14 AM	$1,032.15	$1,044.54	$12.39

Table summarizing the transactions described in paragraph 39.

38. Based on your affiant's knowledge of SNAP trafficking patterns, AHM and the SNAP eligible items within the store, the average transaction amount for medium grocery stores in Guilford County, and general life experience shopping for groceries, your affiant believes these EBT transactions are fraudulent. This is based on your affiant's belief that it is unlikely that an EBT cardholder purchased $1,032.15 or $2,492.95 worth of items at AHM; it is unlikely that AHM could ring up and process $1,032.15 worth of items through their checkout in two minutes and eight seconds; it is unlikely that a cardholder could shop for $1,032.15 worth of SNAP eligible items after learning their balance, or reduce or add items from their already selected items to total within two-percent of their available SNAP balance.

Piggyback Transactions

39. Your affiant knows from training and experience conducting SNAP trafficking investigations that retailers often conduct fraudulent trafficking transactions shortly after smaller SNAP transactions. While the reasoning behind this belief is unknown to your affiant, transactions matching this pattern have been discovered in nearly every store suspected of SNAP trafficking that your affiant has examined and is common enough that FNS has developed a transactions filter that sorts through store transaction data to identify these "piggyback transactions." Your affiant has located transactions patterns consistent with this methodology of trafficking.

40. On December 11, 2021, two transactions were conducted at AHM consistent with the "piggyback transactions" pattern:

a. On December 11, 2021, at 11:22:30 AM, an EBT card was swiped through AHM's POS terminal for a $3.99 transaction.

b. One minute and thirty-two seconds later, at 11:24:02 AM, a Nevada-issued EBT card was manually inputted into AHM's POS terminal for a $975.81 transaction.

41. As described in paragraph 18, an EBT transaction conducted by manually inputting the EBT card's number into a POS terminal is often an indicator of fraudulent EBT transactions. An EBT card issued from another state being manually inputted into a POS terminal is a second indicator of fraudulent EBT transactions.

42. Additional transactions matching this pattern with the same Nevada-issued EBT card were located in AHM's transactional history, which along with the transaction detailed above, are summarized in the table below:

Date	Time	Amount	Issuing State	Transaction Method
12/11/2021	11:22:30 AM	$3.99	North Carolina	Swipe
12/11/2021	11:24:02 AM	$975.81	Nevada	Manual
08/06/2022	04:11:21 PM	$31.59	North Carolina	Swipe
08/06/2022	04:13:37 PM	$749.68	Nevada	Manual
10/05/2022	01:34:59 PM	$10.00	North Carolina	Manual
10/05/2022	01:36:52 PM	$1,209.15	Nevada	Manual
05/05/2023	05:45:54 PM	$31.82	North Carolina	Swipe
05/05/2023	05:48:27 PM	$1,170.12	Nevada	Manual

Table summarizing the transaction described in paragraph 42, as well as other similar transactions not detailed above. Other transactions involving the Nevada-issued card were located but not included in this table.

43. This pattern was identified in other transactions not involving the Nevada-issued EBT card. On August 25, 2021, the following two transactions occurred:

a. On August 25, 2021, at 11:39:38 AM, an EBT card was swiped through AHM's POS terminal for a $209.70 transaction.

b. Two minutes and fifty-two seconds later, at 11:42:30 AM, a different EBT card was manually inputted into AHM's POS terminal for a $1,603.21 transaction.

44. On February 11, 2024, the following two transactions occurred:

a. On February 11, 2024, at 06:18:32 PM, an EBT card was swiped through AHM's POS terminal for a $28.01 transaction.

b. Two minutes and four seconds later, at 06:20:36 PM, a different EBT card was swiped through AHM's POS terminal for a $750.25 transaction.

Interstate Nature of SNAP Trafficking

45. Your affiant examined the SNAP transactional history throughout the United States for the aforementioned Nevada-issued EBT card and determined the card was first utilized at AHM on November 3, 2021, and that it was most recently utilized at AHM on November 6, 2024.

46. During this same approximately three-year period, the Nevada EBT card has redeemed a total of $48,672.82 in SNAP benefits over 268 transactions throughout the United States. Of those 268 transactions, 217 occurred in Nevada and two of them occurred in Arizona, all of which were completed by the EBT card being swiped through a POS terminal.

47. The remaining 49 transactions were conducted at AHM in North Carolina, all of which were conducted by manually inputting the EBT card number into the POS terminal. These 49 manual transactions at AHM totaled approximately $32,594.31 in SNAP transactions, or 66.97% of the Nevada card's SNAP redemption during this time period.

48. During this same time period, the 35 largest EBT transactions conducted by the Nevada EBT card were all at AHM, ranging from $1,298.41 to $450.25. Setting aside transactions conducted at AHM, the subject card had only three transactions greater than $300.00; the remaining 216 non-AHM transactions were all less than $294.00.

49. Some transactions and the subsequent transactions in other states occurred too close in time for the cardholder to have legitimately traveled between the two SNAP retailers. For example, on March 5, 2023, two manually inputted transactions occurred at AHM, at 05:53:50 PM and 05:57:15 PM for $912.49 and $391.08, respectively. Thirty-minutes and two seconds later, a

$6.43 transaction in which the EBT card was swiped at a POS terminal of a store in Nevada occurred.

50. Based on the foregoing, your affiant believes all of the SNAP redemptions made by the subject Nevada EBT card at AHM are fraudulent SNAP trafficking transactions.

B. Investigative Activity

51. Around July 2024, the High Point Police Department (hereinafter "HPPD") and your affiant discussed AHM's alleged SNAP trafficking, and later opened a joint investigation between HPPD and USDA-OIG.

52. During this investigation, SNAP trafficking transactions have been conducted at AHM by undercover law enforcement officers (hereinafter "UC"). Your affiant obtained undercover EBT cards, indistinguishable from standard EBT cards, that were loaded with SNAP benefit funds and provided them to HPPD for use by the UC.

53. KHAN completed ten SNAP trafficking transactions, providing the UC with cash in exchange for SNAP benefits that were processed through the POS terminal in AHM. KHAN charged the UC a fee each time. The UC purchased items from AHM's inventory during each undercover transaction, some of which were ineligible items as described in paragraphs 13 and 14.

54. During these undercover transactions, $4,676.06 of SNAP benefits were spent at AHM, $4,360.00 of which were SNAP benefits trafficked by KHAN. These transactions are summarized in the table below.

Date	EBT Transaction Amount	Cash Received by UC	Fee Charged by AHM
08/12/24	$85.19	$40.00	$20.00
08/15/24	$147.37	$80.00	$40.00
08/21/24	$130.82	$60.00	$40.00
09/03/24	$1,148.10	$800.00	$320.00
09/10/24	$223.18	$140.00	$60.00
09/18/24	$307.87	$200.00	$80.00
09/24/24	$884.79	$600.00	$260.00

10/01/24	$316.18	$200.00	$80.00
10/16/24	$182.48	$100.00	$40.00
11/12/24	$599.94	$400.00	$180.00
01/02/25	$650.14	$400.00	$220.00

EBT Transactions Total	$4,676.06
Fees Total	$1,340.00
Cash Received	$3,020.00
SNAP Benefits Trafficked	**$4,360.00**

Table comparing summarizing the undercover SNAP trafficking transactions conducted by HPPD and USDA-OIG at AHM. The "SNAP Benefits Trafficked" total is the sum of the "Cash Received by UC" and "Fee Charged by AHM"

55. During the undercover transactions, the UC observed different locations from which KHAN would retrieve the cash paid to the UC. In most undercover transactions, KHAN would retrieve cash from under the counter at the checkout of AHM.

56. During the undercover transaction that occurred on January 2, 2025, the UC observed KHAN remove a "roll" of cash from his pocket to pay the UC the cash for the trafficking transaction. The UC estimated that the "roll" could have been $10,000 to $15,000 based on its size.

SNAP Trafficking Transaction Witnessed by UC

57. On August 26, 2024, HPPD told your affiant that the UC observed a suspicious interaction inside APH between KHAN and a customer that may have been related to SNAP trafficking while the UC was conducting an undercover transaction themselves. The UC observed the customer enter AHM and walk directly towards KHAN at the cash register and ask if they could 'have 60 today.' The UC did not observe what occurred after this as they moved to a different part of the store. The UC subsequently completed an undercover SNAP trafficking transaction with KHAN.

58. Your affiant examined AHM's SNAP transaction data to see if the suspicious interaction described above resulted in a trafficking transaction. Not knowing if this suspicious interaction observed by the UC occurred during the August 15, 2024, or August 21, 2024,

undercover transactions at AHM, your affiant examined the data for both dates. This review of data revealed that on both dates, the EBT transactions proceeding the undercover trafficking transactions by the UC appeared to also be SNAP trafficking transactions. Further analysis of the cards used in the proceeding trafficking transactions revealed a history of trafficking SNAP benefits at AHM over the course of multiple years.

59. The data for the SNAP recipient account associated with the EBT card used in the transaction immediately preceding the undercover trafficking transaction completed on August 15, 2024, indicated that the recipient had been trafficking their SNAP benefits at AHM for multiple years. Starting as early as December 11, 2021, and through at least January 11, 2025, this recipient conducted 36 transactions at AHM totaling $5,916.92, all of which your affiant believes were SNAP trafficking transactions. This belief is based on the transactional history of the subject account at AHM and indicators of fraudulent transactions, which includes manual transactions and balance depletions, as described in paragraphs 18 and 34, respectively. Additionally, a review of the subject accounts shows that the account has its SNAP benefits reloaded onto the EBT card on the 11th of each month, and 21 of the 36 transactions at AHM described above occurred on the 11th day of the month.

60. The following table exhibits 14 of the 34 transactions conducted at AHM by the subject account as representative sample. Your affiant believes all 34 transactions were SNAP trafficking transactions.

Date	Amount	Prior Balance	% Balance Depletion	Transaction Method
12/11/21	$201.10	$251.08	80.09%	Manual
12/25/21	$97.06	$97.38	99.67%	Manual
04/11/22	$213.79	$214.30	99.76%	Manual
11/13/22	$202.71	$206.95	97.95%	Manual
12/11/22	$281.11	$281.66	99.80%	Swipe
01/11/23	$202.09	$281.43	71.81%	Swipe
03/11/23	$196.78	$196.81	99.98%	Swipe

04/11/23	$199.05	$199.11	99.97%	Swipe
05/11/23	$201.31	$215.50	93.42%	Swipe
06/11/23	$202.79	$281.07	72.15%	Swipe
01/11/24	$204.16	$221.98	91.97%	Swipe
05/11/24	$261.33	$293.08	89.17%	Swipe
08/15/24	$121.10	$146.30	82.78%	Swipe
01/11/25	$160.32	$296.40	54.09%	Swipe

Table displaying 14 of the transactions conducted by the subject SNAP account at AHM. The SNAP trafficking transaction that occurred on August 15, 2024, is the EBT transaction immediately preceding the undercover SNAP trafficking transaction.

61. A review of the transactional history of the EBT card used in the SNAP trafficking transaction that occurred before the UC's undercover SNAP trafficking transaction on August 21, 2024, revealed a history of fraudulent transactions at AHM. Much like the account analyzed in the preceding two paragraphs, this EBT card has a history of balance depletion transactions, manual transactions, the majority of which also occurred on the same day the account receives its monthly benefits, the 21st of each month. The subject EBT card conducted 11 transactions at AHM, nine of which occurred on the same day of the month that the account received its benefits. The cumulative total of these 11 transactions at AHM is $2,555.67.

62. The following table exhibits all 11 of the transactions conducted at AHM by the subject account. Your affiant believes all 11 transactions were SNAP trafficking transactions.

Date	Amount	Prior Balance	% Balance Depletion	Transaction Method
10/25/23	$401.92	$427.69	93.97%	Swipe
02/21/24	$232.14	$233.00	99.63%	Swipe
03/21/24	$204.91	$233.00	87.94%	Swipe
04/19/24	$155.11	$155.58	99.70%	Swipe
05/21/24	$221.32	$222.45	99.49%	Swipe
06/21/24	$201.01	$234.13	85.85%	Swipe
07/21/24	$221.13	$234.00	94.50%	Swipe
08/21/24	$216.11	$233.39	92.60%	Swipe
10/21/24	$236.02	$236.28	99.89%	Manual
12/21/24	$233.97	$234.00	99.99%	Manual
01/21/25	$232.03	$234.03	99.15%	Manual

Table displaying the 11 conducted by the subject SNAP account at AHM. The SNAP trafficking transaction that occurred on August 21, 2024, is the EBT transaction immediately preceding the undercover SNAP trafficking transaction.

VII. FACTUAL BASIS FOR SEIZING ITEMS

63. Your affiant knows from training and experience, and the collective experience of other law enforcement officers involved in this investigation, that retail food stores such as Apna Halal Meats frequently maintain the following records and other items that constitute evidence, proceeds and/or instrumentalities of SNAP fraud, or that other entities may hold these records, such as security surveillance store. These include:

64. **Sales, purchase and inventory records.** Retail food stores must maintain records to facilitate the operation of the business. Product invoices and inventory records detailing the volume of wholesale food purchased by the store can be compared to the corresponding retail sales negotiated using SNAP benefits. A comparison of these figures would reveal whether a particular store had adequate eligible inventory to support the volume of items that store employees purportedly sold with SNAP benefits.

65. **POS devices and receipts.** Investigative operations and USDA records have shown that the owners and employees of AHM used at least one unique POS terminal during the course of this investigation. POS devices are an instrumentality for committing SNAP fraud since they provide the means to conduct transactions that result in funds transfers. Terminals located in the store can serve as corroborating evidence for suspected fraudulent transactions detected by the ALERT system.

66. **EBT cards.** EBT cards are an instrumentality for committing SNAP fraud as they provide the means to access funds allocated to individual recipient accounts. Retailers engaged in SNAP fraud frequently retain recipients' EBT cards in the store to conduct multiple low dollar

amount transactions over an extended period of time. Such transactions are less likely to be flagged as fraudulent.

67. **United States Currency.** U.S. Currency is both an instrumentality for committing SNAP fraud and proceeds of the offense. A review of ALERT data disclosed that from April 2018 through the end of October 2024, AHM conducted approximately 16,300 transactions that match known patterns of illegal SNAP benefits trafficking that USDA computer systems have flagged and identified, some of which are detailed in this affidavit. AHM's SNAP benefits redemption total for October 2024 was $59,129.69. Trafficking benefits at a rate of approximately $59,129.69 per month requires cash on hand of approximately $29,564.85 per month, or approximately $953 per day. Additionally, the undercover law enforcement conducting SNAP trafficking transaction with KHAN witnessed KHAN remove a "roll" of cash from his pocket to pay the UC for one of the trafficking transactions.

68. **Records pertaining to the exchange of cash for SNAP benefits.** Retailers engaged in SNAP fraud frequently maintain records of their illicit transactions. Owners or employees commonly maintain ledgers, telephone books, address books, or lists of names to document with whom they conduct transactions and the number of benefits they purchase.

69. **Records pertaining to assets.** Individuals and businesses engaged in financial crimes frequently convert criminally derived proceeds into tangible assets such as vehicles, real property, commercial goods, and investments. These assets are eligible for seizure and forfeiture. In addition, records of their acquisition may demonstrate the intent to conceal proceeds and/or further the criminal scheme.

70. **Financial transaction records.** Bank records and similar documents may serve as evidence of SNAP fraud and/or conversion of criminally derived proceeds into assets. As outlined

previously, SNAP transactions are conducted via electronic funds transfer, similar to the process employed with credit and debit cards. SNAP transactions records maintained by FNS and FIS may be compared with bank records to trace the movement of proceeds.

71. **Safety deposit box records and keys.** Individuals and businesses engaged in financial crimes also frequently convert criminally derived proceeds into bulk cash. Safety deposit boxes are commonly used as secure storage for large amounts of currency.

72. **Tax returns.** Corporate tax returns contain information that may be used to demonstrate intent to conceal criminal activity and associated proceeds. Net sales, gross income, and cost of goods sold may be compared with summary SNAP redemption data to reveal significant discrepancies. Additionally, corporate tax returns can contain relevant information for identifying assets derived with criminal proceeds.

73. **Store security video footage.** During the course of this investigation, HPPD determined that AHM utilizes a video surveillance security system. These systems are commonly digital video recorders ("DVR"s). A comparison of store surveillance footage with SNAP transaction data could identify video footage of likely fraudulent transactions.

Computers and Computer Data

74. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

75. **Probable cause.** Your affiant knows from training and experience that owners and operators of retail food stores use electronic records and communications to facilitate business operations. Further, your affiant knows that an email address was listed on AHM's FNS Form 252 that was submitted during the application to become an approved SNAP retailer. A different email address is listed in the current contact information for the AHM's owner, KHAN, in FNS databases. Furthermore, on a daily basis, SNAP funds are transferred to the repository bank account for AHM, which results in online banking actions. Additionally, FNS records indicate that the initial application by KHAN for AHM to become a SNAP retailer were made online. This evidence suggests the use of one or more computers to conduct business at AHM and the SUBJECT PREMISES.

76. The trafficking of benefits from cards located out of state, such as the trafficking transactions with the Nevada-issued EBT card described in paragraphs 42 through 45, performed by manually inputting the EBT card's number and PIN indicate that the EBT card was not present at AHM, and imply some sort of coordinating communication with the cardholder (or whoever was in possession of the card). Based on your affiant's experience in conducting SNAP trafficking transactions and common familiarity with communication methods utilized individuals, these communications likely occurred via cell phone. This same concept applies to any transactions processed via manually inputted card numbers, regardless of the state of issue. The manual input indicates that the EBT card is not present at AHM, and that KHAN or another individual at AHM are communicating with the cardholder (or whoever was in possession of the card) and coordinating the trafficking transactions. At the time this affidavit was authored, the most recent transactional data available to your affiant was through February 1, 2025. A manual transaction depleting 90.75% of an Illinois issued EBT occurred on February 1, 2025.

77. Based on my knowledge, experience, and training, your affiant submits that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons: Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

78. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

79. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

80. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

81. **Forensic evidence.** As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES for at least the following reasons:

82. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

83. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and

durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it pertains to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning),

or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

84. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

85. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

86. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

87. **Necessity of seizing or copying entire computers or storage media.** In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either

seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

88. **The time required for an examination.** As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

89. **Technical requirements.** Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

90. **Variety of forms of electronic media.** Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

91. **Nature of examination.** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

92. **Necessity of retaining forensic images for purposes of authentication at trial**. In anticipation of litigation relating to the authenticity of data seized pursuant to the warrant, the government requests that it be allowed to retain a digital copy of all seized information authorized by the warrants for as long as is necessary for authentication purposes.

93. In light of these concerns, I hereby request the Court's permission to search, copy, image and seize the computer hardware (and associated peripherals) that are believed to contain some or all of the evidence described in the warrants, and to conduct an off-site search of the image or hardware for the evidence described.

Biometric Unlocking

94. I am further seeking permission, pursuant to these warrants to permit law enforcement to, using a device's biometric features, compel KHAN to unlock any cellular devices located on the premises. I seek this authority based on the following:

95. From training and experience, I know that users of cellular devices also carry their cellular devices on their persons or keep them in close proximity so they can access them.

96. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices,

particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

97. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the font of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

98. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

99. If a device equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises

by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates and infrared-sensitive camera to record data based on patterns within the user's irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

100. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a number or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

101. As discussed in this affidavit, I have reason to believe that KHAN uses a cellular device(s) in connection with SNAP trafficking activities and that such cellular device will be found during a search of the SUBJECT PREMISES. The passcode or password that would unlock the cellular device subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within such devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

102. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a

fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement discover that the device is locked and equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

103. Based on the foregoing, if law enforcement personnel encounter a cellular device and the phone may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from KHAN, the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the device, including to (1) press or swipe the fingers (including thumbs) of the aforementioned person to the fingerprint scanner of the device; (2) hold the device in front of the face of KHAN to activate the facial recognition feature; and/or (3) hold the device in front of the face of KHAN to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

104. The proposed warrant does not authorize law enforcement to require that KHAN state or otherwise provide the password or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the device and any other electronic device seized from KHAN'S person. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person would be permitted under the proposed warrant. To avoid confusion on that point, if agents

in executing the warrant ask KHAN for the passwords to a device, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the cellular device, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

CONCLUSION

105. Based on the above, I believe there is probable cause to find that violations of 7 U.S.C. § 2024; 18 U.S.C. § 1029; 18 U.S.C. § 641; and 18 U.S.C. § 1343 occurred, and that evidence of such violations (described in Attachment B) will be found at the SUBJECT PREMISES.

106. Based upon the foregoing, I request that this Court issue the proposed search warrant, pursuant to Federal Rule of Criminal Procedure 41, to allow the search of the SUBJECT PREMISES more particularly described in Attachment A, and the seizure of the items described in Attachment B.

107. I declare under the penalty of perjury under the laws of the United States that the foregoing is true and correct.

/s/ Michael Johnson by LPA

Michael Johnson
Special Agent, USDA-OIG

Pursuant to Rule 4.1 of the Federal Rules of Criminal Procedure, the affiant appeared before me via reliable electronic means (telephone), was placed under oath, and attested to the contents of this written affidavit.

03/04/25

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The place to be searched is 2610 Plaza Court, #107, High Point, North Carolina 27263 (SUBJECT PREMISES), further described as a unit within a commercial property located in Guilford County, North Carolina, with Guilford County Parcel Number 179411 and PIN 7709739123. The SUBJECT PREMISES is a light-colored single story commercial building, with a unit number of #107. The SUBJECT PREMISES has signage above the doors and windows that reads "Apna Halal Meats" in red letters. The dual doors to enter the SUBJECT PREMISES have an 'OPEN' sign above them. The windows running a portion of the length of the building facing Plaza Court have signage advertising items, one of which reads "Fresh Meats Goat Chicken Lamb Beef."

The place to be searched includes the interior of the SUBJECT PREMISES and any part of the property inside the SUBJECT PREMISES. Two photographs of the SUBJECT PREMISES are shown below.

The SUBJECT PREMISES viewed from the publicly accessible area in front of the building.

The SUBJECT PREMISES viewed from the publicly accessible area in front of the building.

ATTACHMENT B

Items to be seized referencing or revealing fraud associated with the Supplemental Nutrition Assistance Program

Evidence of violations of 7 U.S.C. § 2024; 18 U.S.C. § 1029; 18 U.S.C. § 641; and 18 U.S.C. § 1343, namely:

1. Sales, purchase and inventory records for the corporation PAK MK FAMILY, Inc., Apna Halal Meats, or any entity believed to be associated with PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and the SUBJECT PREMISES.

2. Point-of-sale devices and receipts generated by point-of-sale devices.

3. Supplemental Nutrition Assistance Program (SNAP) Electronic Benefit Transfer (EBT) cards.

4. United States Currency.

5. Records that pertain to the exchange of cash for SNAP benefits, including ledgers, telephone, address books, and lists of names.

6. Records that pertain to assets held by PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and any entity associated with SUBJECT PREMISES, which were derived or maintained with proceeds from the criminal acts listed in this affidavit.

7. Records of financial transactions which were conducted by PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and any entity associated with SUBJECT PREMISES, including bank statements, check stubs or registers, canceled checks, deposit tickets, debit memos, credit memos, wire transfer documents, records of savings accounts including passbooks and statements.

8. All records and documents identifying the location of safety deposit boxes or other possible depositories for suspected unlawfully obtained cash and other liquid assets which are

identified in any way with PAK MK FAMILY, Inc., Apna Halal Meats, and any entity associated with SUBJECT PREMISES, namely Mohammad Azam KHAN, as well as other owners, officers, shareholders, agents, and employees, and any keys or other access devices associated with such depositories.

9. All tax returns for PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and any entity associated with SUBJECT PREMISES.

10. Any store security video footage, to include the entire recording system if it is a digital video recorder (DVR) or Network DVR.

11. Computer equipment, electronic storage devices, cellular phones, and electronic media associated with the operation of PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and any entity associated with SUBJECT PREMISES. Electronic devices, including but not limited to central processing units; desktop computers, laptop computers, mobile devices, notebooks, and tablet computers; personal digital assistants; peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, USB flash drives, thumb-drives, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices, but only as to electronic devices and other digital devices for which it is determined that complete images of such devices cannot successfully be made during execution of the warrant.

12. All passwords, passphrases, encryption keys, encryption dongles, and/or any information including tools, records, and techniques used the data stored within electronic devices that have been used or may have been used to store the records and things described below.

13. All passwords, passphrases, encryption keys, encryption dongles, and/or any information including tools, records, and techniques used to activate and/or navigate and access in plain-text data stored in encrypted data systems, encrypted file systems, encrypted files, and encrypted records or documents.

14. Training materials, including training manuals, examples, templates and correspondence in electronic, video, and paper formats.

15. Internal memos, directives, emails, and any other correspondence between Mohammad Azam KHAN and employees of PAK MK FAMILY, Inc., Apna Halal Meats, and any entity associated with SUBJECT PREMISES relating to procedures for handling SNAP transactions.

16. Corporate documents of PAK MK FAMILY, Inc., including the articles of incorporation, corporate minutes, financial records including bank account records, receipts, ledgers, cash receipt books, statements, bank books, check books, payroll records.

17. Financial business records for PAK MK FAMILY, Inc., Apna Halal Meats, Mohammad Azam KHAN, and any entity associated with SUBJECT PREMISES, including bank account records, deposit statements/slips, receipts, checks, ledgers, cash receipt books, bank statements, bank books, check books, check registers, savings pass books, withdrawal slips, Certificate of Deposit (CD) documents, wire transfers, cashier's checks, money orders, financial statements, credit applications, loan documents, loan payments, loan statements, invoices and/or bills, payroll records, currency, safe deposit box records and keys.

18. For electronic devices or storage media whose seizure is otherwise authorized by this warrant, and electronic storage media or digital devices that contain or in which there are stored records or information that is otherwise called for by this warrant (hereinafter, "DEVICE"):

a. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;

f. evidence of the times the DEVICE was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the DEVICE;

h. documentation and manuals that may be necessary to access the DEVICE or to conduct a forensic examination of the DEVICE; and

i. records of or information about Internet Protocol addresses used by the DEVICE.

19. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any

form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; and

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately referencing or revealing the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

20. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the

attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

DEVICE UNLOCK: During the execution of the search of the SUBJECT PREMISES, law enforcement personnel are authorized to unlock any seized electronic communication device by (1) pressing or swiping the fingers (including thumbs) of **KHAN** to the fingerprint scanner of the device; (2) holding the device in front of the face of **KHAN** to activate the facial recognition feature; and/or (3) holding the device in front of the face of **KHAN** to activate the iris recognition feature, for the purpose of attempting to unlock the device and attempting to access data contained in the device in order to search the contents as authorized by this warrant.